REMARKS

In accordance with the foregoing, claims 1, 8-11, and 16 are amended. Claims 1-19 are pending and under consideration. No new matter is presented in any of the foregoing and, accordingly, approval and entry of the amended claims are respectfully requested.

Statement On Substance Of Interview

An interview was conducted between the Applicant's representative and the Examiner on September 27, 2005. Features that patentably distinguish aspects of the present invention over the cited art were discussed. Other arguments presented are discussed below. Applicant thanks the examiner for the opportunity to conduct the in-person interview.

Claim Amendments

Claims 1 and 8-10 are amended, using claim 1 as an example, to respectively recite a data generating apparatus and a computer-readable storage medium, and a method "generating a plurality of random numbers based on the inputted condition, generating a plurality of candidates for expression data of the finite field by using the generated random numbers, and checking whether each of the candidates applies to the expression data of the finite field; and . . . storing candidates which apply to the expression data of the finite field. "

Claim 11 is amended to recite a data generating apparatus wherein "the expression data is based on random numbers generated that are based on the inputted condition."

Claim 16 is amended to recite a method "generating a plurality of random numbers based on the designated condition; generating expression data of the finite field based on the generated random numbers."

As discussed during the in-person interview, no new matter is presented in any of the foregoing and, accordingly, approval and entry of the amended claims are respectfully requested.

Traverse Of Rejections

The Examiner rejects claims 1-3, 6-12, and 14-19 under §103(a) as unpatentable over Leppek (U.S.P. 5,933,501) in view of Schneier (Applied Cryptography, 1996, pages 584 and 320), and claims 4-5 and 13 under 35 U.S.C. §103(a) as unpatentable over Leppek in view of Wright Paper A Random Polynomial Generator, July 14, 1994, Pages 1-9).

Features Recited By Claims Not Taught By Cited Art

Independent claims 1 and 8-10, all as amended, respectively recite, using claim 1 as an example, a data generating apparatus, a computer-readable storage medium, and a method "generating a plurality of random numbers based on the inputted condition, generating a plurality

of candidates for expression data of the finite field by using the generated random numbers, and checking whether each of the candidates applies to the expression data of the finite field; and . . . storing candidates which apply to the expression data of the finite field. "

Independent claim 11, as amended, recites a data generating apparatus wherein "the expression data is based on random numbers generated that are based on the inputted condition."

Independent claim 16, as amended, recites a method "generating a plurality of random numbers based on the designated condition; generating expression data of the finite field based on the generated random numbers."

As discussed during the in-person interview and agreed by the Examiner, none of the cited art alone or in combination, teach for example, a first "generating a plurality of random numbers based on the inputted condition" and then a second "generating a plurality of candidates for expression data of the finite field by using the generated random numbers" as recited by the claims according to aspects of the present invention.

Further, as discussed during the in-person interview, none of the cited art further checks whether "each of the candidates applies to the expression data of the finite field."

The Action further concedes that Leppek does not teach "details that would indicate that the PGP algorithm whose conditions are of a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as prime number and a positive integer indicating an extension degree, respectively." (Action at page 3).

In addition, Applicant respectfully submits that chance occurrences as taught by Schneier do not teach features as recited by claims of the present invention, in which, in response to an input for specifying a bit length, a finite field expression is returned by extracting a prime number that is expressed in this specified bit length from a table or by generating a prime number having this specified bit length.

Further, since in a case of the IDEA algorithm as taught by Schneier, an *arguendo* "finite field" is unchangeable, Applicant submits that a proposed combination by the Examiner teaches away from recited features, using claim 1 as an example, of "inputting a condition specified by a user for designating a finite field."

Further, dependent claims recite features not taught by he cited art, alone or in combination. As an example, claim 4 recites an apparatus " wherein when the extension degree is inputted as the condition, said generation device automatically generates irreducible

polynomial data corresponding to the extension degree and stores the irreducible polynomial data in said expression data storage device.

Even an *arguendo* combination does not teach features recited by claims 4, 5, and 13 since a polynomial generated taught by Wright has coefficients that are assigned in a random manner. That is, Wright teaches a method that is different from and does not teach an irreducible polynomial according to an aspect of the present invention.

As provided in MPEP §2143.03 "To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F. 2d 1981, (CCPA 1974)." Accordingly, Applicant submits that *prima facie* obviousness is not established.

No Motivation To Combine The Art In A Manner As Suggested By The Examiner

As discussed during the in-person interview, Applicant submits that there is no stated motivation to combine the art as the Examiner contends. The Examiner's contention that a motivation exists since a reference "A "does not have details and a reference "B" has details is an omnibus type of rejection. As set forth in MPEP §707.07 entitled Completeness and Clarity of Examiner's Actions such a rejection should be avoided. Using the Examiner's circular logic, a motivation exists to combine any two references, being different, since the references are by nature different.

Further, Applicant submits there is no motivation to modify Leppek with Wright merely because Wright is "already been proven," as the Examiner contends. (Action at page 7). As set forth in MPEP §2144. 04:

> (t)he mere fact that a worker in the art could rearrange the parts of the reference device . . . is not by itself sufficient to support a finding of obviousness. The prior art must provide a motivation . . . without the benefit of appellant's specification, to make the necessary changes in the reference device.

Accordingly, Applicant submits that *prima facie* obviousness is not established.

Cited Art Is Nonanalogous Art

As set forth in MPEP §2141.01(a) entitled Analogous and Nonanalogous Art that analogous art "is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering his problem."

In the Advisory Action mailed January 28, 2005, the Examiner states the "combination of Schneier and Leppek are analogous art because Schneier teaches the instances when the encryption operator of Leek have a finite field."

Applicant submits that the Examiner's contention is incorrect, since none of the cited art

teach "inputting a condition for designating a finite field" or "automatically generating expression data of the finite field based on the inputted condition." (Emphasis added).

Applicant submits that the Examiner is mistaken in this contention and that with respect to the three operations taught by Schneier on page 320, paragraph 2, XOR and addition modulo $2^{16} + 1$ have nothing to do with the finite field operations, whatsoever.

Summary

Since features recited by claims 1-19 are not taught by the cited art, alone or in combination, there is no motivation to combine the references in a manner as suggested by the Examiner, and *prima facie* obviousness is not established, the rejection should be withdrawn and claims 1-19 allowed.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: October 19, 2005

By: Paul W. Bobowiec

Paul W. Bobowiec
Registration No. 47,431

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501